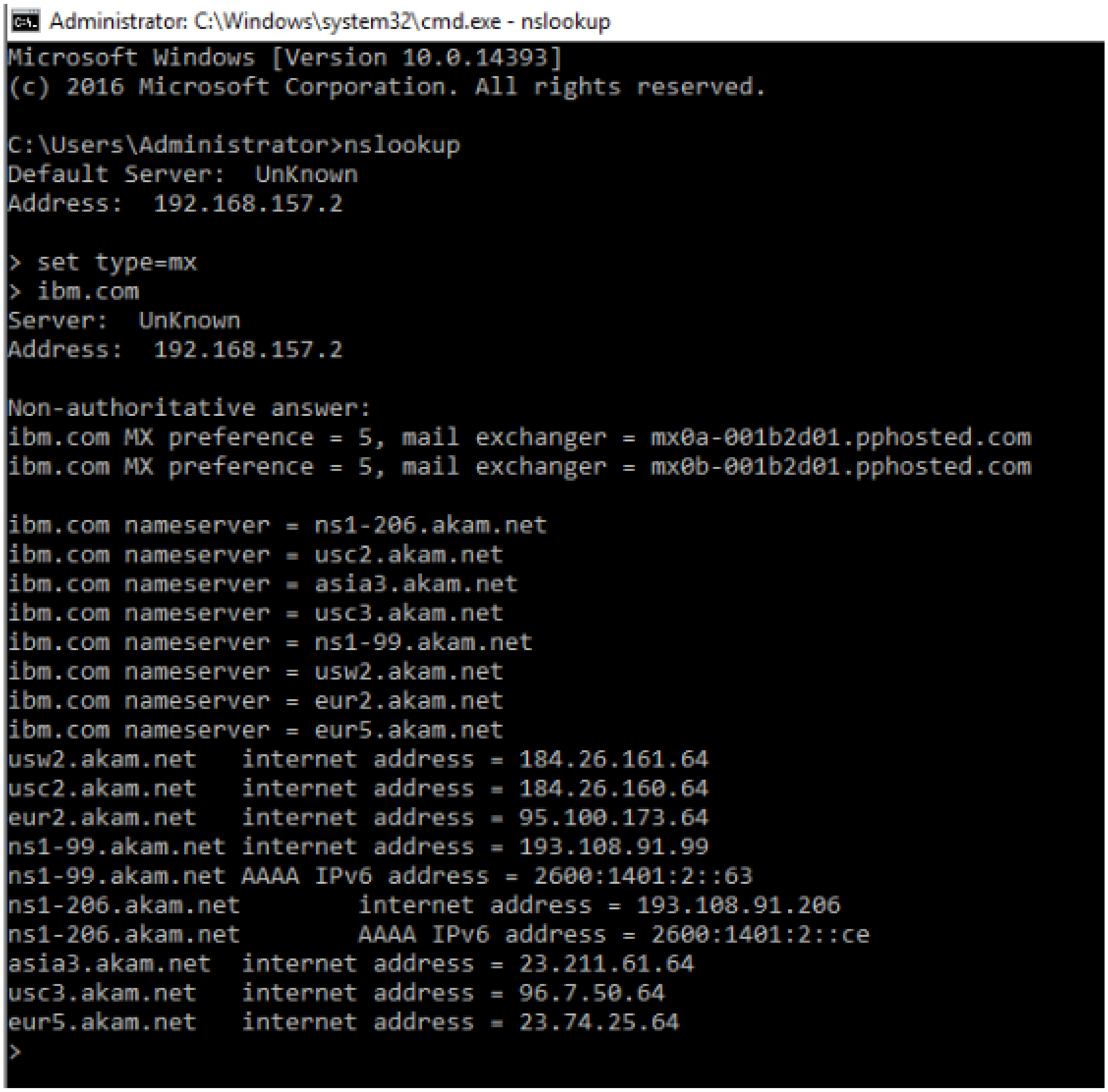
DAY 4 ASSIGNMENT:

question 1:

Find out the mail servers of the following domain:

- Open Windows Server 2016 VM image and open terminal window by typing cmd in windows run window (win+R).
- Type the command 'nslookup'.
- Now for find mail servers for domain set the parameter type by the command 'set type=mx'.
- Then type ibm.com and wipro.com to enlist their respective mail servers.
- Entries with MX preference would provide details of mail servers.

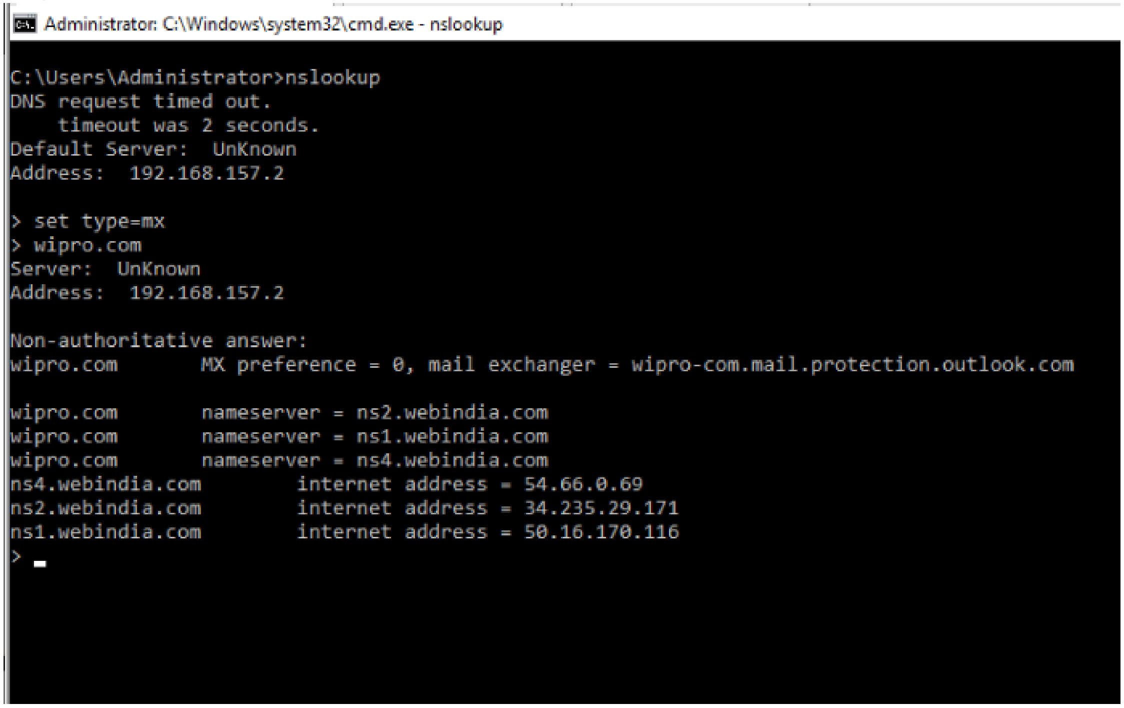
Ibm.com



Administrator: C:\Windows\system32\cmd.exe - nslookup

```
Microsoft Windows [Version 10.0.14393]
(c) 2016 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>nslookup
Default Server:  UnKnown
Address:  192.168.157.2

> set type=mx
> ibm.com
Server:  UnKnown
Address:  192.168.157.2

Non-authoritative answer:
ibm.com MX preference = 5, mail exchanger = mx0a-001b2d01.pphosted.com
ibm.com MX preference = 5, mail exchanger = mx0b-001b2d01.pphosted.com

ibm.com nameserver = ns1-206.akam.net
ibm.com nameserver = usc2.akam.net
ibm.com nameserver = asia3.akam.net
ibm.com nameserver = usc3.akam.net
ibm.com nameserver = ns1-99.akam.net
ibm.com nameserver = usw2.akam.net
ibm.com nameserver = eur2.akam.net
ibm.com nameserver = eur5.akam.net
usw2.akam.net   internet address = 184.26.161.64
usc2.akam.net   internet address = 184.26.160.64
eur2.akam.net   internet address = 95.100.173.64
ns1-99.akam.net internet address = 193.108.91.99
ns1-99.akam.net AAAA IPv6 address = 2600:1401:2::63
ns1-206.akam.net        internet address = 193.108.91.206
ns1-206.akam.net        AAAA IPv6 address = 2600:1401:2::ce
asia3.akam.net  internet address = 23.211.61.64
usc3.akam.net   internet address = 96.7.50.64
eur5.akam.net   internet address = 23.74.25.64
>
```

Wipro.com



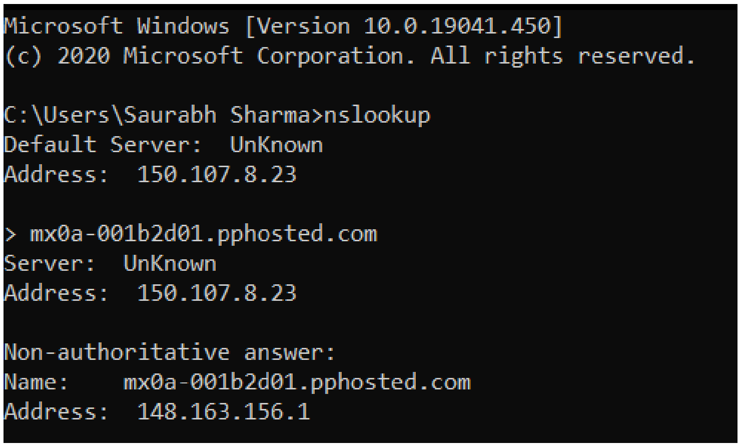
Administrator: C:\Windows\system32\cmd.exe - nslookup

```
C:\Users\Administrator>nslookup
DNS request timed out.
    timeout was 2 seconds.
Default Server:  UnKnown
Address:  192.168.157.2

> set type=mx
> wipro.com
Server:  UnKnown
Address:  192.168.157.2

Non-authoritative answer:
wipro.com       MX preference = 0, mail exchanger = wipro-com.mail.protection.outlook.com

wipro.com       nameserver = ns2.webindia.com
wipro.com       nameserver = ns1.webindia.com
wipro.com       nameserver = ns4.webindia.com
ns4.webindia.com        internet address = 54.66.0.69
ns2.webindia.com        internet address = 34.235.29.171
ns1.webindia.com        internet address = 50.16.170.116
> _
```

question 2:
Find the locations, where these email servers are hosted.

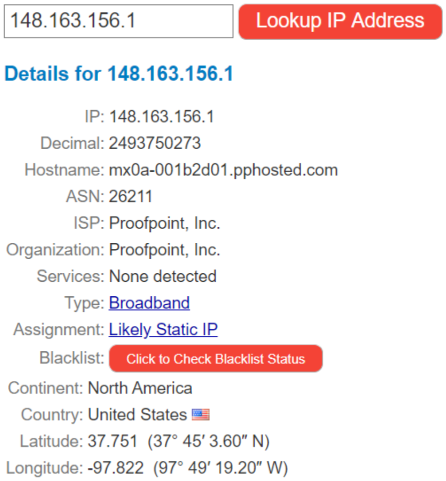
We can locate the IP for email server domain using the domain name from above results. And the from online IP lookup website we can find locations of these IP addresses

For IBM:

1. 

```
Microsoft Windows [Version 10.0.19041.450]
(c) 2020 Microsoft Corporation. All rights reserved.

C:\Users\Saurabh Sharma>nslookup
Default Server:  UnKnown
Address:  150.107.8.23

> mx0a-001b2d01.pphosted.com
Server:  UnKnown
Address:  150.107.8.23

Non-authoritative answer:
Name:    mx0a-001b2d01.pphosted.com
Address:  148.163.156.1
```

2.



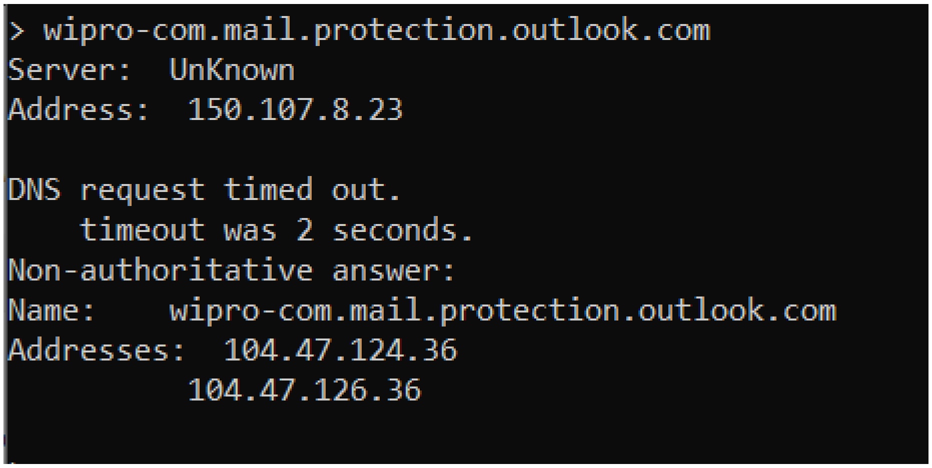
148.163.156.1

Details for 148.163.156.1

IP: 148.163.156.1
Decimal: 2493750273
Hostname: mx0a-001b2d01.pphosted.com
ASN: 26211
ISP: Proofpoint, Inc.
Organization: Proofpoint, Inc.
Services: None detected
Type: Broadband
Assignment: Likely Static IP
Blacklist:
Continent: North America
Country: United States
Latitude: 37.751 (37° 45′ 3.60″ N)
Longitude: -97.822 (97° 49′ 19.20″ W)

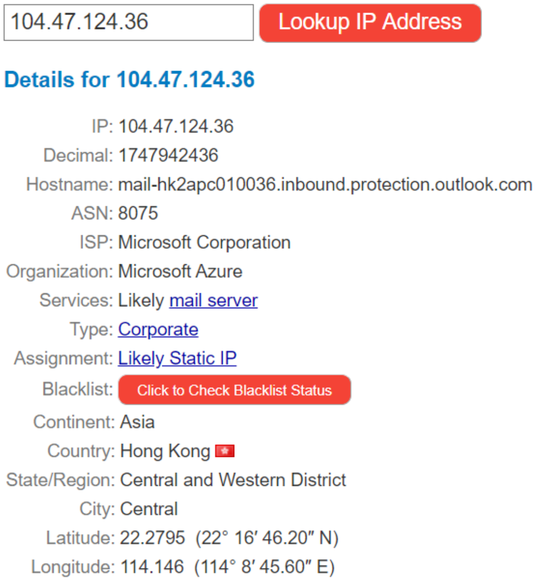
For wipro:

1.



```
> wipro-com.mail.protection.outlook.com
Server:  UnKnown
Address:  150.107.8.23

DNS request timed out.
    timeout was 2 seconds.
Non-authoritative answer:
Name:    wipro-com.mail.protection.outlook.com
Addresses:  104.47.124.36
          104.47.126.36
```

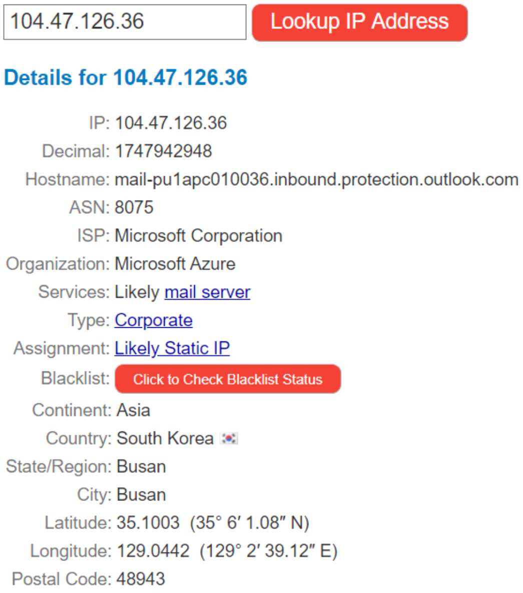
2.



104.47.124.36

Details for 104.47.124.36

IP: 104.47.124.36
Decimal: 1747942436
Hostname: mail-hk2apc010036.inbound.protection.outlook.com
ASN: 8075
ISP: Microsoft Corporation
Organization: Microsoft Azure
Services: Likely mail server
Type: Corporate
Assignment: Likely Static IP
Blacklist:
Continent: Asia
Country: Hong Kong
State/Region: Central and Western District
City: Central
Latitude: 22.2795 (22° 16′ 46.20″ N)
Longitude: 114.146 (114° 8′ 45.60″ E)



104.47.126.36

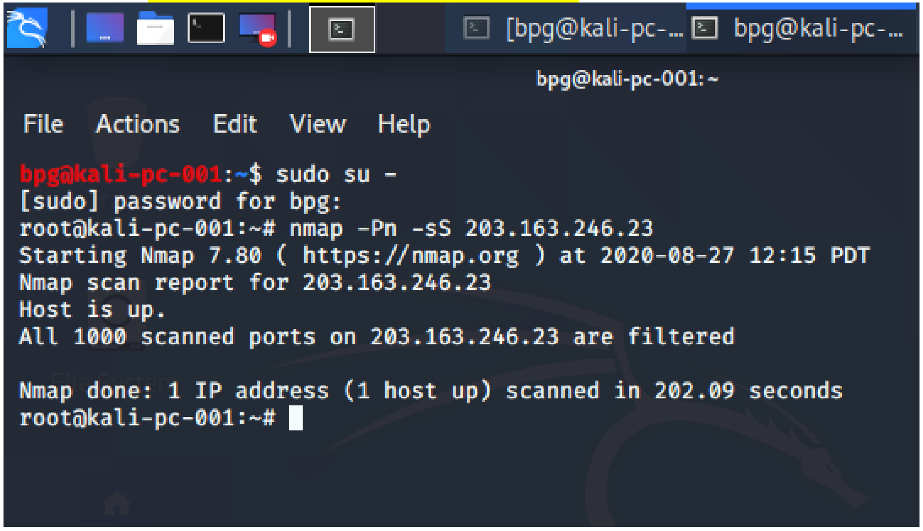
Details for 104.47.126.36

IP: 104.47.126.36
Decimal: 1747942948
Hostname: mail-pu1apc010036.inbound.protection.outlook.com
ASN: 8075
ISP: Microsoft Corporation
Organization: Microsoft Azure
Services: Likely mail server
Type: Corporate
Assignment: Likely Static IP
Blacklist:
Continent: Asia
Country: South Korea
State/Region: Busan
City: Busan
Latitude: 35.1003 (35° 6′ 1.08″ N)
Longitude: 129.0442 (129° 2′ 39.12″ E)
Postal Code: 48943

question 3:

Scan and find out port numbers open 203.163.246.23

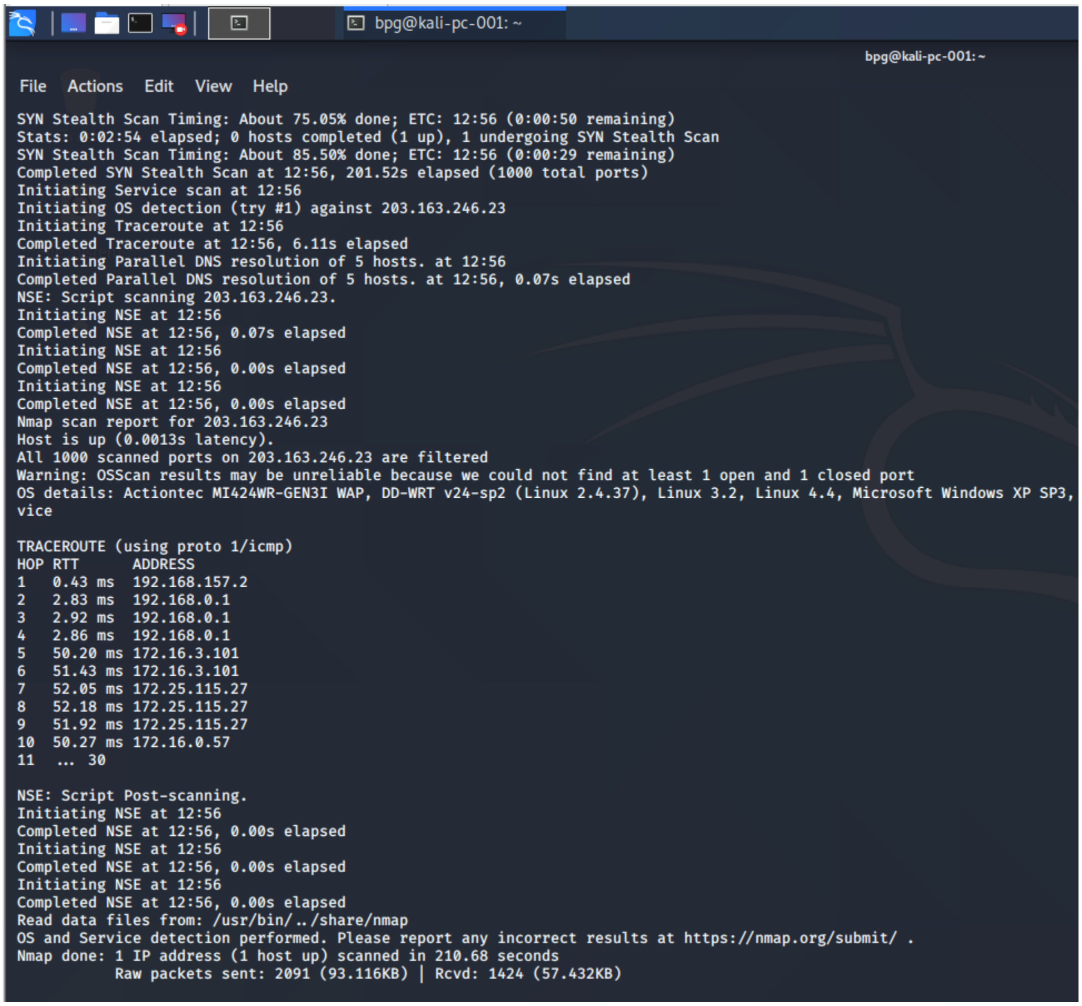
- First one KALI Linux VM and then open terminal.
- Change to root user by the command ‘sudo su –‘ and then enter password for current user.
- Now type the following command for Nmap to lookup all the ports of given IP and tell their status.
  - Nmap -Pn -sS 203.163.246.23



```
bpg@kali-pc-001:~$ sudo su -
[sudo] password for bpg:
root@kali-pc-001:~# nmap -Pn -sS 203.163.246.23
Starting Nmap 7.80 ( https://nmap.org ) at 2020-08-27 12:15 PDT
Nmap scan report for 203.163.246.23
Host is up.
All 1000 scanned ports on 203.163.246.23 are filtered

Nmap done: 1 IP address (1 host up) scanned in 202.09 seconds
root@kali-pc-001:~#
```

Same response even with stealth scan:

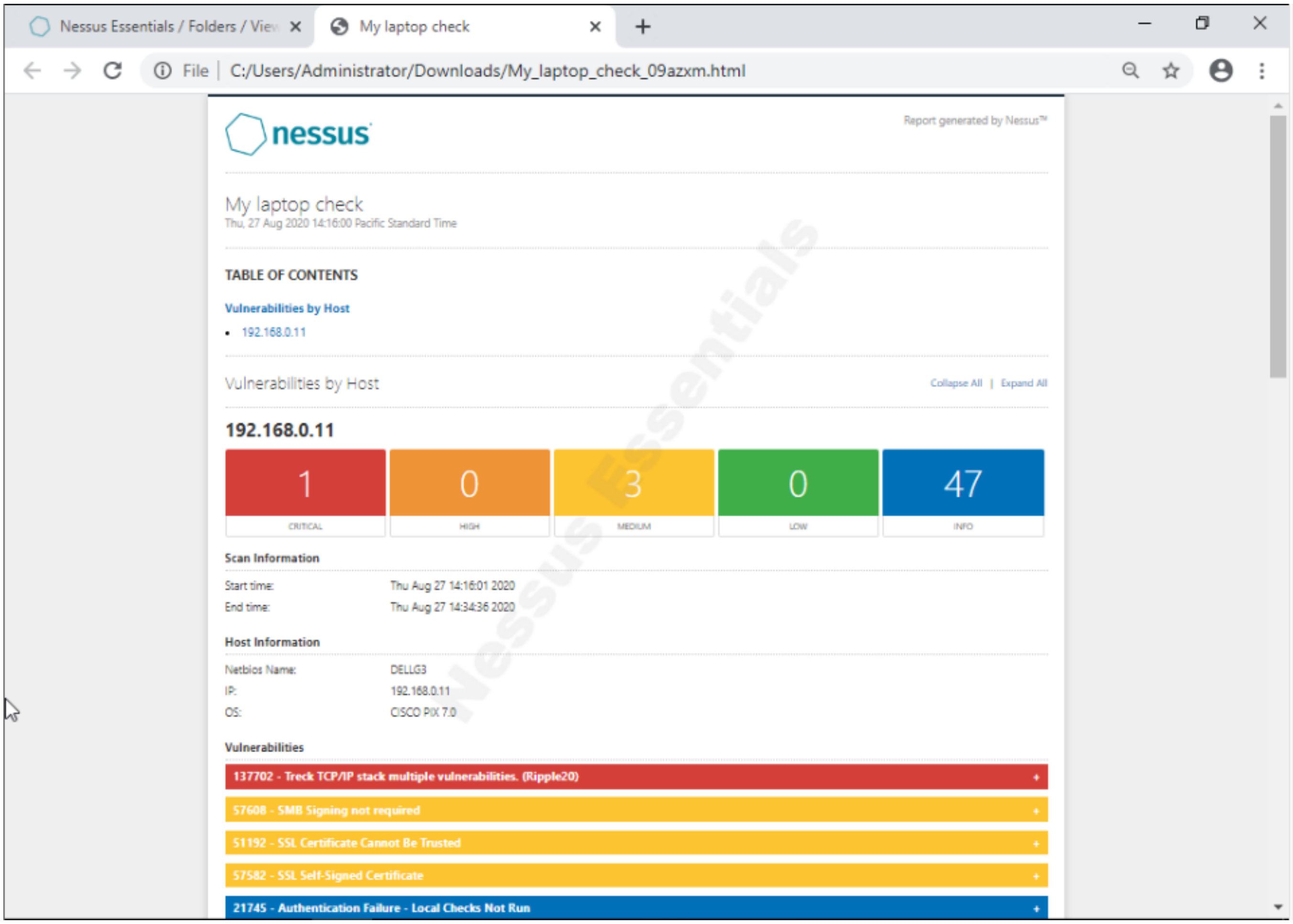
- Nmap -Pn -sS -A -v 203.163.246.23



```
SYN Stealth Scan Timing: About 75.05% done; ETC: 12:56 (0:00:50 remaining)
Stats: 0:02:54 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 85.50% done; ETC: 12:56 (0:00:29 remaining)
Completed SYN Stealth Scan at 12:56, 201.52s elapsed (1000 total ports)
Initiating Service scan at 12:56
Initiating OS detection (try #1) against 203.163.246.23
Initiating Traceroute at 12:56
Completed Traceroute at 12:56, 6.11s elapsed
Initiating Parallel DNS resolution of 5 hosts. at 12:56
Completed Parallel DNS resolution of 5 hosts. at 12:56, 0.07s elapsed
NSE: Script scanning 203.163.246.23.
Initiating NSE at 12:56
Completed NSE at 12:56, 0.07s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Nmap scan report for 203.163.246.23
Host is up (0.0013s latency).
All 1000 scanned ports on 203.163.246.23 are filtered
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
OS details: Actiontec MI424WR-GEN3I WAP, DD-WRT v24-sp2 (Linux 2.4.37), Linux 3.2, Linux 4.4, Microsoft Windows XP SP3,
vice

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   0.43 ms  192.168.157.2
2   2.83 ms  192.168.0.1
3   2.92 ms  192.168.0.1
4   2.86 ms  192.168.0.1
5   50.20 ms 172.16.3.101
6   51.43 ms 172.16.3.101
7   52.05 ms 172.25.115.27
8   52.18 ms 172.25.115.27
9   51.92 ms 172.25.115.27
10  50.27 ms 172.16.0.57
11   ... 30

NSE: Script Post-scanning.
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Initiating NSE at 12:56
Completed NSE at 12:56, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 210.68 seconds
           Raw packets sent: 2091 (93.116KB) | Rcvd: 1424 (57.432KB)
```

question 4:

Install nessus in a VM and scan your laptop/desktop for CVE.


Nessus Essentials / Folders / View
My laptop check
File
C:/Users/Administrator/Downloads/My_laptop_check_09azxm.html
nessus
Report generated by Nessus™
Nessus Essentials

My laptop check
Thu, 27 Aug 2020 14:16:00 Pacific Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.0.11

Vulnerabilities by Host

Collapse All | Expand All

192.168.0.11

1	0	3	0	47
CRITICAL	HIGH	MEDIUM	LOW	INFO

Scan Information

Start time:	Thu Aug 27 14:16:01 2020
End time:	Thu Aug 27 14:34:36 2020

Host Information

Netbios Name:	DELLG3
IP:	192.168.0.11
OS:	CISCO PIX 7.0

Vulnerabilities

- 137702 - Treck TCP/IP stack multiple vulnerabilities. (Ripple20) +
- 57608 - SMB Signing not required +
- 51192 - SSL Certificate Cannot Be Trusted +
- 57582 - SSL Self-Signed Certificate +
- 21745 - Authentication Failure - Local Checks Not Run +